CERT
Software Engineering Institute
Carnegie Mellon University

TUNISIA CSIRT CASE STUDY

The CSIRT Development and Training team has published this case study—part of a series of case studies—to assist CSIRTs in getting started and improving their performance.

Introduction

Tunisia is acutely aware of its location at the crossroads of Europe, Africa, and the Middle East, as shown by this slide taken from a presentation by tunCERT, which is proud of its status as the first FIRST team in Africa.

FIRST Teams around the world
By countries
By team name
189 Teams across 41 countries

Like the rest of the world, Tunisia experienced explosive growth in internet service after the turn of the century, growing from 200 web sites in 1999 to 6,200 in 2008, and from 150,000 users to 2,600,000 users during that same period. Perhaps even more important is that the number of ISPs more than doubled, growing from 616 in 1999 to 1,548 in 2006.

Relationships

The Tunisian government CSIRT is tunCERT. Prior to 2009, the name had been CERT-TCC, where "TCC" stood for "Tunisian Coordination Center." Although a "micro-CERT" had been in place since 1999, it was not until 2004 that CERT-TCC was formed by the National Agency for Computer Security, or NACS, the high-level ICT Security organization in Tunisia.

Although a national team, tunCERT feels it has a regional avocation. It is the first African CERT to be accepted into FIRST, to which it has belonged since 2007. It is a UNCTAD (United Nations Conference on Trade and Development) center of excellence, and since 2006 has been the secretary of the Organization of the Islamic Conference's OIC-CERT.

Approach

The tunCERT began in 1999 with a very small team of three or four people dedicated to combating the threats to the country's booming internet. The Y2K phenomenon had created a crisis atmosphere that catalyzed their operations.

From the beginning, the Tunisian team realized it needed a pragmatic approach to confront what it calls the three lacks: lack of awareness, lack of experts, and lack of money. The team developed a three-pronged attack. It began by raising the awareness of politicians and policymakers, which led to some short-term loans and technical assistance. This let its members to turn their attention to the IT management community, which set up a task force of local experts to develop the training needed to solve the lack of expertise. Finally they were ready to establish a national strategy for dealing with information security problems.

Decision Makers

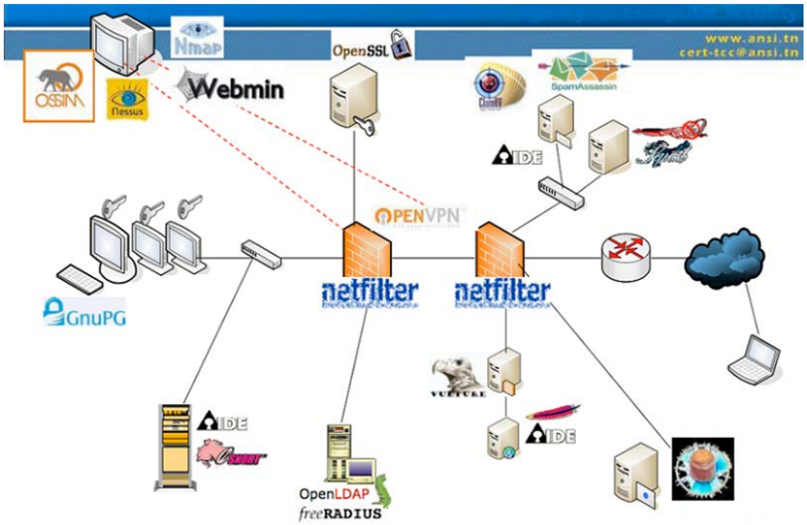
Early on, the Tunisian team realized that decision makers were key people for promoting a culture of IT security within the nation. The team developed an awareness campaign for those decision makers that included a "hacking exposed" demonstration, which was apparently an eye opener and allowed the decision makers to get in touch with the reality of the risks.

The team feels that its approach paid off by leading to a series of strong laws on IT security, which greatly facilitated their growth. This legislation started with a law against cybercrime in 1999, a law on e-commerce in 2000, and two very important laws in 2004: a law on the protection of privacy and personal data and a law on computer security that instituted a security audit program and established the NACS.

CISOs and Professionals

From there the team turned its attention to the CISOs and the professionals with an information and assistance program that collects and disseminates information through multiple channels, including mailing lists, a website, brochures, knowledgebases, and news. The team currently offers more than 30 guides and manuals on topics such as best practices, security policies, technical tips, acquisition, etc. It also sponsors a variety of special events, such as a CISO day that draws more than 140 CISOs to discuss new attacks, technologies, and tools; an IT security auditor day that attracts more than 160 auditors to share standards, methodologies, and problems; a software developer's day; and the tunCERT Forum.

One aspect that sets tunCERT apart is its focus on open source tools, which it sees as an important way of dealing with the "lack of money" problem. Its staff defined a three-phase plan that started by providing support for the deployment of existing open source tools, continued through the customization of open-source solutions for specific clients, and is now in the third phase, which is the launch of real research and development of new open source tools. tunCERT currently has five federated R&D projects under the supervision of the Ministry of Scientific Research, and is launching a World-Bank-funded research laboratory specializing in open source security tools.



The Internet Community

Having addressed the decision makers and the professional community, tunCERT was ready to reach out to the broader internet community. It developed four CD-ROMs of awareness material, an information security calendar, eight awareness brochures, and several awareness posters. It works actively with the media to provide them the information they need to raise the awareness of the broader population, to the extent that tunCERT has a dedicated press-relations position. It participates weekly in eight national radio programs, and twice monthly in a TV program.

It also works with the schools to get the message out. It has prepared a packet of awareness courses for the primary schools, developed cartoons and games for children, and provided web-based materials for parents as well as children.

The team also works with higher education and the training community. They developed a Masters program in IT security, which was launched in 2004. By 2008, it had produced eight Master's graduates. They have worked with ISC2 and ISACA to facilitate advanced IT security courses in Tunisia.

Finally, tunCERT works with non-governmental organizations and associations. It participates in the National Internet Festival, organizes awareness activities in cooperation with the Association Tunisienne d'Internet et Multimédia, and attends more than 20 national seminars and workshops per year. It participated in the formation of an academic association for IT security (the Tunisian Association for Numeric Security) as well as a professional association (the Tunisian Association of Experts in Computer Security). It is working on an association of ISPs as well.

Most recently, tunCERT has begun to take an active role in international cybersecurity. In August 2008, it set forth a plan to develop a regional CERT for Eastern and Southern Africa based on its own experience.

Conclusion

The Tunisian experience illustrates many of the issues and themes of developing national teams: funding issues and creative solutions such as focusing on open source; the importance of sponsorship from the top, in this case the politicians; identifying the constituency; building relationships; developing expertise when necessary; and starting small.

References

[CONP 2010]
"Lineamientos de política ara ciberdefensa". Consejo Nacional de Política Económica Social, República de Colombia, Departamento Nacional de Planeación draft document, 2010.

[CONP 2011]
"Lineamientos de política ara ciberdefensa". Consejo Nacional de Política Económicay Social, República e Colombia, Departamento Nacional de Planeación document Conpes 3701, 2011.

[DURA 2011]
Duran Santos, Alex. "Policia Nacional: Evolución de la Ciberseguridad CSIRT-PONAL." ARADI-PONAL, Bogotá, 2011.

[MINI 2008]
Ministerio de Comunicaciones, República e Colombia, "Diseño de un CSIRT de Colombia para la estrategia Gobierno en Linea." Bogotá, December 2008.

[NOTI 2010]
Noticias de Colombia, "Ministerio de Defensa implementa centro contra ataques cibernéticos," 2010.

[SALA 2011]
Salas, F. C. "El Gobierno en línea y la seguridad de la información". Presentation at the International Seminar on Information Security "Nuevos Retos", Bogotá, Colombia, October 2011.

[TUNI 2005]
"Tunis Agenda for the Information Society". International Telecommunications Union Document WSIS-05/TUNIS/DOC/6 (Rev. 1)-E, Tunis, November, 2005.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0004353